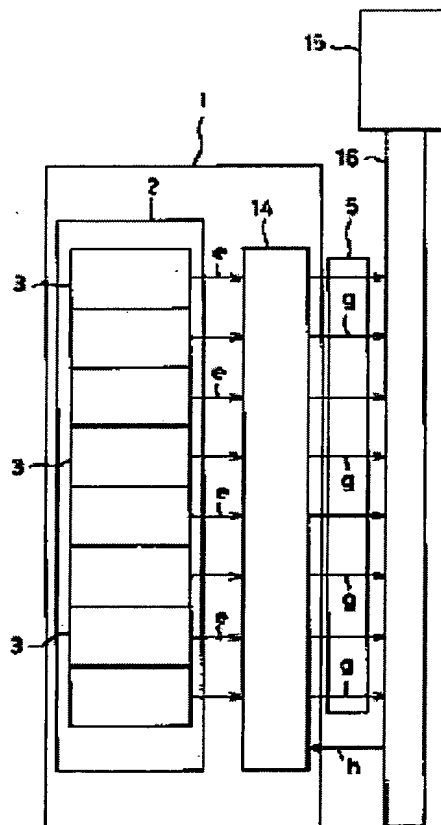


**8-BIT RANDOM NUMBER GENERATOR**

Patent number: JP9097170  
Publication date: 1997-04-08  
Inventor: ITO TORU  
Applicant: NIKO DENSHI KK  
Classification:  
- International: G06F7/58  
- european:  
Application number: JP19950255217 19951002  
Priority number(s): JP19950255217 19951002

**Abstract of JP9097170**

**PROBLEM TO BE SOLVED:** To directly obtain and output an 8-bit random number signal from a binary random number generator. **SOLUTION:** This generator consists of an 8-bit random number generation part 2 where eight random number generation circuits 3 which output random number signals (e) obtained by digitizing a noise signal (a) are provided in parallel and an 8-bit parallel transmission part 14 which takes individual random number signals (e) as the input and obtains a binarized signal (g) by sampling respective random number signals (e) at the same point of time in accordance with a control signal (h) from the outside and outputs this signal (g) as an 8-bit random number output (f), thus generating the 8-bit random number output (f) easy to handle at an 8-fold conversional speed of the speed before.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-97170

(43) 公開日 平成9年(1997)4月8日

(51) Int.Cl.<sup>6</sup>

G 0 6 F 7/58

識別記号

庁内整理番号

F I

G 0 6 F 7/58

技術表示箇所

A

審査請求 未請求 請求項の数 2 O L (全 5 頁)

(21) 出願番号 特願平7-255217  
(22) 出願日 平成7年(1995)10月2日

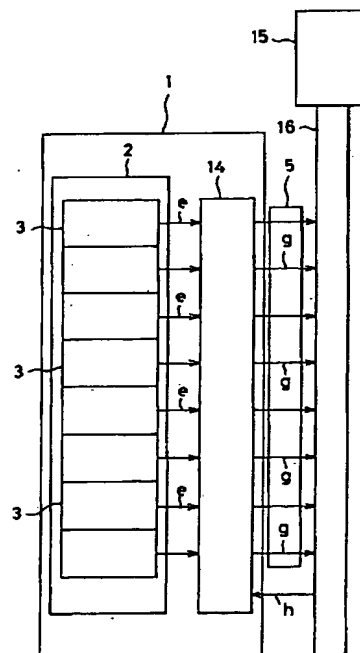
(71) 出願人 391044292  
ニコー電子株式会社  
神奈川県横浜市港北区太尾町910番  
(72) 発明者 伊東 徹  
神奈川県横浜市港北区太尾町910番地 ニ  
コー電子株式会社内  
(74) 代理人 弁理士 渡辺 一豊

(54) 【発明の名称】 8ビット乱数作成装置

(57) 【要約】

【課題】 2進乱数作成装置から、直接に8ビットの乱数信号を得て、出力することにある。

【解決手段】 雑音信号aをデジタル化した乱数信号eを出力する8つの乱数発生回路3を並列に設けた8ビット乱数発生部2と、各乱数信号eを個々に入力して、外部からの制御信号hに従って各乱数信号eを同一時点でサンプリングして得た2値化信号gを8ビット乱数出力fとして出力する8ビット並列送出部14とから構成し、従来の8倍の速度で取り扱いの便利な8ビット乱数出力fを作成する。



## 【特許請求の範囲】

【請求項1】 直流成分を除去した確率的特性が既知であると共に、所定の帯域に制限されたガウス性電気雑音信号(a)をデジタル化した2進乱数信号(e)を出力する8つの乱数発生回路(3)を並列に設けた8ビット乱数発生部(2)と、該8ビット乱数発生部(2)の各乱数発生回路(3)からの乱数信号(e)を個々に入力し、演算装置(15)からの制御信号(h)に従って、前記各乱数信号(e)を単一のサンプリングパルスでサンプリングして得た2値化信号(g)を8ビット乱数出力(f)として演算装置バス(16)に出力する8ビット並列送出部(14)と、から成る8ビット乱数作成装置。

【請求項2】 各乱数発生回路(3)におけるガウス性電気雑音信号(a)の発生源を、ノイズツェナーダイオード(5)とした請求項1記載の8ビット乱数作成装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、システムのランダムデータによるシュミレーション、システムパラメタのランダムな選択、或いはデジタル情報のランダムな符号変換等に利用される8ビット乱数作成装置に関するものである。

## 【0002】

【従来の技術】例えば、ノイズツェナーダイオードからの電子雪崩効果によって生成される電気雑音信号は、極めて低い周波数(10Hz程度)から数10MHz帯程度まで電力スペクトラムが平坦なガウス性白色雑音であることが知られており、これを利用したアナログ雑音発生器が通信回線の情報伝送品質の特性試験等に使用されている。

【0003】このアナログ雑音発生器からの出力信号はアナログ波形であるので、デジタル的信号の取扱いが主流となっている現在、システムパラメタのランダムな選択、デジタル情報のランダムな符号変換等への応用には、更に何らかの変換が必要である。

【0004】この要望を満たすべく、確率的特性の既知であり、かつ所定の帯域に制限された電気雑音信号から、1と0の2値系列から成るデジタル形式の乱数信号を得る技術が提案され、2進乱数作成装置として、暗号化用の乱数鍵やパスワード等の作成のために使用されている。

## 【0005】

【発明が解決しようとする課題】しかしながら、従来の2進乱数作成装置により、コンピュータ等の演算装置で最も処理のし易い8ビットの乱数信号を得るには、2進乱数作成装置から出力された乱数信号を8回繰り返してサンプリングしなければならず、8ビットの乱数信号を得るのに面倒な手間と処理とが必要であると云う問題があった。

【0006】また、従来の2進乱数作成装置が発生する

乱数信号の速度は、最高で10MHzであるため、発生する乱数信号の波長に近い速度でサンプリングすると、同一波長内の値をサンプリングする場合が生じ、サンプリングした値がランダムではなくなってしまうことを考慮して、乱数信号発生速度よりも或る程度低い速度でサンプリングを行う必要があり、このため8ビットの乱数信号を作成するには、1ビットの場合の8倍以上の時間が必要となると云う問題があった。

【0007】すなわち、図6に示すように、一つの乱数発生回路3で構成された2進乱数作成装置から出力された一つの乱数信号eから8ビット乱数出力を得るには、図7に示すように、出力された乱数信号eを第1のサンプリングパルスb1から第8のサンプリングパルスb8により1ビット毎の直列採取を行う必要があり、サンプリングパルスbによる採取を開始してから、サンプリングパルスbの時間間隔の少なくとも8倍の時間後の第8のサンプリングパルスb8による採取が完了した時点で、8ビット乱数出力(図7の場合、[10011101]、16進数では9D)を得ることになり、各サンプリングパルスbのサンプリングにより得た2値化信号を順に記憶する回路構成を必要とすることになっていた。

【0008】そこで、本発明は、上記した従来技術における問題点を解消すべく創案されたもので、2進乱数作成装置から直接8ビットの乱数信号を得ることを技術的課題とし、もって演算装置における乱数信号の利用を容易なものとすると共に、速やかに円滑な乱数信号利用状況を得ることを目的とする。

## 【0009】

【課題を解決するための手段】上記技術的課題を解決するため、本発明のうち、請求項1記載の発明は、直流成分を除去した確率的特性が既知であると共に、所定の帯域に制限されたガウス性電気雑音信号aをデジタル化した2進乱数信号eを出力する8つの乱数発生回路を並列に設けた8ビット乱数発生部を有すること、この8ビット乱数発生部の各乱数発生回路からの乱数信号eを個々に入力し、演算装置からの制御信号hに従って、各乱数信号eを単一のサンプリングパルスでサンプリングして得た2値化信号gを8ビット乱数出力fとして演算装置バスに出力する8ビット並列送出部を有すること、を手段としている。

【0010】請求項2記載の発明は、請求項1記載の発明の構成のうち、各乱数発生回路におけるガウス性電気雑音信号aの発生源を、ノイズツェナーダイオードとしたことを手段としている。

## 【0011】

【作用】請求項1記載の発明は、8つの乱数発生回路を並列に設けて8ビット乱数発生部を構成しており、各乱数発生回路から同期して出力された乱数信号eを、そのまま8ビット並列送出部に入力する。

【0012】8ビット並列送出部は、一種のゲート回路

であって、外部の演算装置からの制御信号hの入力に従って、8ビット乱数発生部から入力された個々の乱数信号eを一つのサンプリングパルスでサンプリングして得た、すなわち1ビットの時間で得た、2値化信号gの組合せとして構成される8ビット乱数出力fを演算装置バスに出力する。

【0013】このように、本発明による8ビット乱数作成装置は、1ビットの時間で、演算装置で処理し易い8ビットの信号である8ビット乱数出力fを演算装置側に出力するので、演算装置側における2値化乱数信号の取り扱いがきわめて容易となると共に、1ビットの時間単位で8ビット乱数出力fを得ることができるので、演算装置側における2値化乱数信号の取り扱い速度を大幅に高めることになる。

【0014】

【実施例】以下、本発明の一実施例を、図1ないし図5を参照しながら説明する。図1は、本発明の8ビット乱数作成装置1の電気的構成の一実施例を示すブロック図で、8ビット乱数発生部2は、8つの乱数発生回路3を並列に設けると共に、各乱数発生回路3からの出力である乱数信号eは、そのまま8ビット乱数発生部2の出力として出力される。

【0015】図2は、乱数発生回路3の電気的構成の一実施例を示すブロック図で、雑音信号発生部4と、A/D変換器10と、信号成形器12とから構成され、一つのサンプリングパルス発生部11が、各乱数発生回路3に接続されている。

【0016】雑音信号発生部4は、電気雑音発生源としてノイズツェナーダイオード5を使用して図3に示す構成となっていて、図3において、6はノイズツェナーダイオード5に電子雪崩を起こすに適切な電流を流すための制限抵抗であり、7は直流分除去用のコンデンサであり、増幅器8の出力端子からノイズツェナーダイオード5から得た雑音信号aが出力される。

【0017】ノイズツェナーダイオード5から得られた雑音信号aは、きわめて低い周波数(10Hz程度)から数10MHz程度までの電力スペクトラムが平坦なガウス性白色雑音であることが知られており、制限抵抗6の抵抗値および印加電圧値を選ぶことにより、通常、数10μAオーダーの電流をノイズツェナーダイオード5の供給電流としている。

【0018】雑音信号発生部4からの雑音信号aは、ローパスフィルタ9により所定の帯域に制限された後、A/D変換器10に入力される。

【0019】A/D変換器10は、入力された雑音信号aをサンプリングパルス発生部11から入力されるサンプリングパルスbでサンプリングし、このサンプリング値をA/D変換する。

【0020】A/D変換器10による雑音信号aのサンプリング値のA/D変換は、A/D変換クロックパルス

によって行われるが、このA/D変換クロックパルスの一つである最小桁クロックパルスdにより、最小桁ビットに生起するデジタル信号である最小桁信号cだけを取り出し、この最小桁信号cを信号成形部12を形成するフリップフロップ回路のS入力に投入する。

【0021】信号成形回路12を形成するフリップフロップ回路のもう一方の入力であるR入力には、A/D変換器10からの最小桁クロックパルスdと最小桁信号cの反転信号とを入力するアンド回路13の出力が入力されるので、信号成形回路12であるフリップフロップ回路は、その出力状態と反対の最小桁信号cが入力される度に、その出力状態を反転させ、これにより2値化系列雑音信号である乱数信号eが生成されて出力される。

【0022】各乱数発生回路3から出力される乱数信号eは、そのまま8ビット乱数発生部2の出力として8ビット並列送出处14に出力されるので、8ビット乱数発生部2の出力信号は8ビット乱数系列となる。

【0023】8ビット並列送出处14は、8ビット乱数発生部2からの出力をそのまま受け入れて、外部からの指令である演算装置15からの制御信号hにより、入力された8つの乱数信号eを単一時点でサンプリングして、各乱数信号eから2値化信号gを生成し、この2値化信号gをそのまま出力することにより、8ビット乱数出力fとして出力する。

【0024】すなわち、図4に示すように、8ビット乱数発生部2の8つの乱数発生回路3から出力された乱数信号eは、図5に示すように、それぞれ同時に8ビット並列送出处14に入力される。

【0025】8ビット並列送出处14に入力された各乱数信号eは、サンプリングパルスとして機能する演算装置15からの制御信号hに従ってサンプリングされて、個々に2値化信号gに生成されると共に、そのまま8ビット乱数出力fとして出力されるが、例えば図5の場合は、第1の制御信号h1により、第1の乱数信号e1から0の2値化信号gが、第2の乱数信号e2から1の2値化信号gが、第3の乱数信号e3から1の2値化信号gが、第4の乱数信号e4から1の2値化信号gが、第5の乱数信号e5から0の2値化信号gが、第6の乱数信号e6から0の2値化信号gが、第7の乱数信号e7から1の2値化信号gが、そして第8の乱数信号e8から1の2値化信号gがそれぞれ得られ、出力される8ビット乱数出力fは〔01110011〕となる。

【0026】この8ビット乱数出力fは、サンプリングパルスとして作用する制御信号hの入力の度に出力されるので、この制御信号hとして従来からのサンプリングパルスを使用することにより、従来の8倍の速度で8ビット乱数出力fを得ることができることになる。

【0027】8ビット並列送出处14から出力された8ビット乱数出力f、すなわち8ビット乱数作成装置1から出力された8ビット乱数出力fは、演算装置15の演

算装置バス16に入力に入力され、そのまま処理される。

【0028】

【発明の効果】本発明は、上記した構成となっているので、以下に示す効果を奏する。8つの乱数信号を一つの信号により単一時点でサンプリングして、各乱数信号を同時に2値化信号に生成し、この8つの2値化信号の組合せを8ビット乱数出力とするので、簡単にかつ正確に8ビット乱数出力を得ることができる。

【0029】生成される8ビット乱数出力は、一つの信号による単一時点でのサンプリングにより得ることができるので、従来の8倍の速度で一つの8ビット乱数出力を得ることができる。

【0030】8ビット乱数出力を直接出力するので、この乱数出力を入力するコンピュータ等の演算装置における8ビット乱数出力の取り扱い処理が容易で簡単なものとなり、きわめて扱い易いものとなる。

【図面の簡単な説明】

【図1】本発明装置の一実施例の電気回路構成を示すブロック図。

【図2】図1に示した実施例における、乱数発生回路の回路構成例を示すブロック図。

【図3】図2に示した乱数発生回路における、雑音信号発生部の回路構成例を示す電気回路図。

【図4】8ビット乱数発生部から並列出力される乱数信号の説明図。

【図5】8ビット並列送出部における8つの乱数信号から8つの2値化信号を生成する動作の説明図。

【図6】従来の乱数作成装置から出力される乱数信号の\*

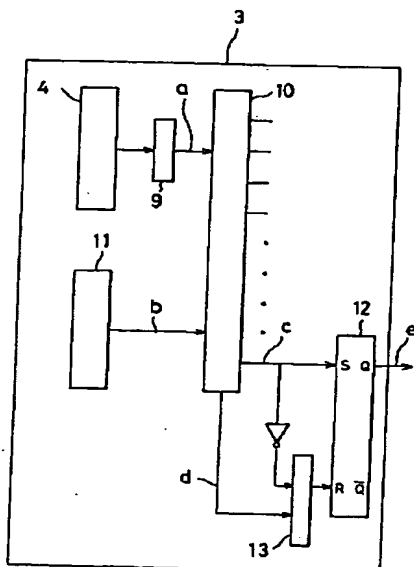
\*説明図。

【図7】図6で得た乱数信号から8ビット乱数出力を得る操作の説明図。

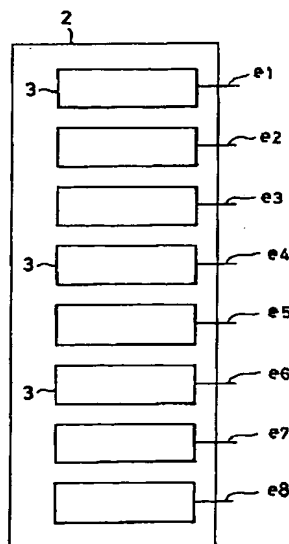
【符号の説明】

- 1 ; 8ビット乱数作成装置
- 2 ; 8ビット乱数発生部
- 3 ; 乱数発生回路
- 4 ; 雑音信号発生部
- 5 ; ノイズツェナーダイオード
- 6 ; 制限抵抗
- 7 ; 直流分カット用コンデンサ
- 8 ; 増幅器
- 9 ; ローパスフィルタ
- 10 ; A/D変換器
- 11 ; サンプリングパルス発生部
- 12 ; 信号成形部
- 13 ; アンド回路
- 14 ; 8ビット並列送出部
- 15 ; 演算装置
- 16 ; 演算装置バス
- a ; 雑音信号
- b ; サンプリングパルス
- c ; 最小桁信号
- d ; 最小桁クロックパルス
- e ; 乱数信号
- f ; 8ビット乱数出力
- g ; 2値化信号
- h ; 制御信号

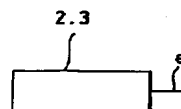
【図2】



【図4】



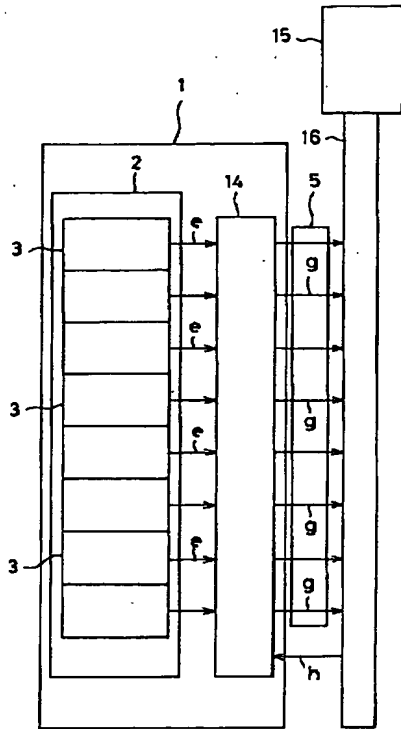
【図6】



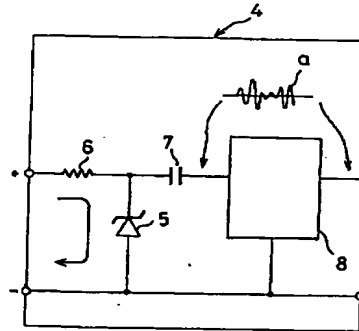
【図7】



【図1】



【図3】



- 1 : 8ビット乱数作成装置    2 : 8ビット乱数発生部    3 : 乱数発生回路  
 4 : 雑音信号発生部    5 : ノイズツェナーダイオード    6 : 無限抵抗  
 7 : 高周波カット用コンデンサ    8 : 増幅器    9 : ローパスフィルタ  
 10 : A/D変換器    11 : サンプルングパルス発生部    12 : 信号成形部  
 13 : アンド回路    14 : 8ビット並列送出部    15 : 演算装置  
 16 : 演算装置バス    a : 雑音信号    b : サンプルングパルス  
 c : 最小桁信号    d : 最小桁クロックパルス    e : 乱数信号  
 f : 8ビット乱数出力    g : 2値化信号    h : 制御信号

【図5】

